STATEMENT OF
JERRY BERMAN
EXECUTIVE DIRECTOR
CENTER FOR DEMOCRACY AND TECHNOLOGY

before the

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION
of the
HOUSE COMMITTEE ON COMMERCE

FEBRUARY 5, 1997

Mr. Chairman and Members of the Subcommittee:

My name is Jerry Berman. I am Executive Director of the Center for Democracy and Technology. The Center is pleased to have this opportunity to address the subcommittee on one of the critical civil liberties issues of our day: the question of privacy in the new communications media, specifically wireless communications.

The Center for Democracy and Technology (CDT) is an independent, non-profit public interest policy organization in Washington, DC. The Center's mission is to develop and implement public policies to protect and advance individual liberty and democratic values in new digital media. The Center achieves its goals through policy development, public education, and coalition building.

The Center coordinates the Digital Privacy and Security Working Group, a diverse coalition of over 50 computer, communications, and public interest organizations working to develop and implement policies that protect personal privacy and network security on the expanding and rapidly changing global information infrastructure. DPSWG originally came into being in 1984 - 1986, when Congress undertook a major review of the federal wiretap laws in order to bring them up to date with advances in technology, including the emergence of wireless communications. DPSWG played a critical role in the enactment of the Electronic Communications Privacy Act of 1986 ("ECPA"). Since then, DPSWG has been involved extensively in the on-going debate over government control of encryption and in the crafting in 1994 of narrowly tailored legislation to preserve law enforcement access to communications while strengthening public accountability mechanisms and

privacy protections, the Communications Assistance for Law Enforcement Act ("CALEA").

Presently, in the belief that the privacy protection laws require periodic review in light of the changing uses of technology, DPSWG is undertaking a major new study of communications privacy, focusing on the effectiveness and coverage of ECPA, implementation of CALEA, the potential of strong encryption technology to protect privacy and security and prevent crime, and other issues. Our study will be completed later this year, but I will share with you today some of our tentative conclusions.

Finally, I should note that one of CDT's priorities has been the promotion of online democracy. CDT is seeking new ways to give Internet users greater access to government and opportunities to participate in the democratic process. To that end, CDT produced the first live cybercast of a congressional hearing which featured realtime interaction between committee members and Internet users. CDT is the coordinator of the Congressional Internet Caucus Advisory Committee, which is working with the Caucus to educate the Congress about the Internet and to expand citizen access to Congress via the Internet. In that regard, we were particularly pleased to see that the Commerce Committee is obtaining testimony in electronic form and posting it on the Committee Website. We congratulate the Committee on this initiative.

I. Ongoing developments in telecommunications increase the urgency of ensuring the privacy and security of wireless communications.

For all the benefits conferred by advancements in communications technology, the American public is deeply concerned that such advancements also threaten to overwhelm the cherished right of privacy. The threats arise from both governmental and private surveillance. Accordingly, for the past thirty years, Congress has recognized that it must ensure that the laws protecting privacy keep pace with the changing uses of technology.

From 1968 when it first enacted the wiretap law known as Title III, through enactment of the Electronic Communications Privacy Act ("ECPA") in 1986, to the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), Congress has sought to balance three goals: (1) to provide strong legal protections for electronic communications, (2) to afford law enforcement

a carefully limited authority to carry out electronic surveillance in serious cases, and (3) to encourage the development and widespread availability of new technologies. ECPA, for example, by extending clear privacy protections to e-mail and cellular telephone conversations, gave an important degree of credibility to those communications media when they were in their infancy, contributing to the dramatic growth they have both undergone.

When it enacted ECPA, Congress knew that it would have to return to the law of communications privacy periodically, as technology continued changing. In that regard, some privacy enhancements were made in CALEA. Now, due to a series of developments, we are at another juncture that requires a major, careful examination of the adequacy of privacy protection legislation. Some of these developments have occurred in the realm of wireless communications: Cellular telephones have become commonplace and are now widely used by ordinary citizens. Moreover, wireless transmission is no longer important only for voice communication, but is becoming increasingly important for data transfer and as the gateway to the global information infrastructure. The Internet has developed since 1986 in ways that the drafters of ECPA never imagined. Telecommunications are becoming increasingly integrated, increasingly global, and increasingly decentralized. These developments, which are central to the ongoing communications revolution, heighten the urgency of ensuring the privacy and security of wireless communications.

In the network of networks that comprise the telecommunications "system" of today and the future, it is no longer appropriate to look at the cellular telephone system as distinct from the wireline system or to look at the telephone system as separate from the Internet. We are seeing a merger of voice, data, and visual communication, carried interoperably over both wireless and wireline means. This integrated network serves a range of commercial, educational, social and political functions. The Internet is a marketplace, a library, a movie theater, a town hall, a social meeting place. Its potential would be stifled equally by excessive government regulation or inadequate privacy and security.

This network knows no national boundaries. Indeed, one of the strengths of the Internet, and one of the ways in which it fosters democratic values, is the ease with which it spans the globe. Information flows as effortlessly from New York to Nairobi as from Washington DC to West

Virginia. Moreover, a communication from New York to Nairobi may travel through the United Kingdom and four other countries one day, but through France and five different countries the next day.

For this reason, it has been said that, on the Internet, the Bill of Rights is a local ordinance. This means that the protections of the US. Constitution offer little privacy assurance to US citizens whose Internet communications regularly cross international borders. Foreign governments can intercept these messages without the knowledge of the senders, and beyond the ability of the US government to protect the privacy of its citizens. Indeed, the US government itself is not bound by requirements of our wiretapping laws when eavesdropping on US citizens from points abroad. The legal scheme of the wiretap laws, as amended by ECPA, should be expanded so that the US government is subject to the court order requirements of the wiretap laws when engaging abroad in surveillance of US citizens for criminal investigative purposes.

With the breakup of telecommunications monopolies, the entry of many new service providers, and the widespread availability of computer technology in the hands of individuals, control over telecommunications technology has become increasingly decentralized. The Internet epitomizes the drive towards decentralization in communications technology.

II. The **privacy of wireless communications is entitled to strong legal protection.**

In this context of a global communications network increasingly dependent on wireless links, we are able to see how it is a serious invasion of privacy to eavesdrop on cellular telephone conversations. Cellular eavesdroppers are invading the privacy not only of the person who is using a cellular phone, but also of anybody else who is on the conversation using an ordinary landline telephone. As cellular telephones become more ubiquitous, cellular scanning threatens the privacy of all telephone users.

Given the growth of wireless services, it is clear that Congress made the right decision in 1986 when it determined that intentionally intercepting cellular phone conversations should be a federal crime. Congress clearly has the authority to protect communications transmitted over the airwaves, and it did so with respect to cellular telephone conversations in ECPA, extending

to the then-fledgling cellular telephone industry the same privacy protections that had applied to traditional wireline services.

ECPA also made it a crime to manufacture, sell, assemble, possess or advertise any device that is "primarily useful" for the interception of wireless telephone conversations. We know that manufacturers, retailers and individuals have taken a very narrow view of this law, and consequently scanners are widely available still that intercept cellular telephones. We believe that the Congress should take a serious look at closing the ambiguities in the scanner law.

III. The privacy of wireless communications goes beyond voice, to the growing area of data communications.

It would be a mistake, however, to limit consideration of wireless communications privacy to voice conversations only, for wireless is becoming increasingly important for data communications. Wireless modems, wireless faxes, and wireless local area networks are linking computers and transferring data that could include proprietary information, medical records, and financial data. Wireless links are becoming more and more important as access points to the global information network.

It is not clear, however, that ECPA clearly protects wireless transfers of data. An earlier industry and privacy task force concluded in 1991 that wireless transfers of data were not covered by ECPA. In 1994, in CALEA and with the support of the Administration, Congress passed a provision making it clear that the privacy of wireless data transfers was protected by ECPA. But less than two years later, in the anti-terrorism act of 1996, Congress repealed the provision. Pub. L. 104-132, section 731.* At a time when wireless local area networks are proliferating and wireless data transmissions could be used for everything from proprietary data to medical records, the law should be

---

* The repeal came at the behest of the Justice Department, which argued that the privacy provision was inappropriately overbroad, and included ham radio and CB radio broadcasts, which should not be privacy-protected. The Justice Department, reversing the Administration's earlier provision, argued that wireless data transfers were already protected. Rather than propose narrower language to make that clear, the Administration successfully argued for repeal of the entire provision. In the context of the many issues in the terrorism bill, this one received little attention.

perfectly clear that wireless data transfers are protected by statute to the same extent as wireless voice communications.

IV. While legal protections are important, they are not enough to ensure privacy. Privacy and security must be ensured through technical means, which the marketplace is developing.

As the recent incident involving the Speaker of the House demonstrates, statutory prohibitions against the interception of cellular phone conversations are not enough. The fact is that devices are still manufactured and marketed that are capable of intercepting cellular telephones, or that can be readily modified to do so, and there are individuals who think it is fun to listen in on other people's cellular telephone conversations.

Again, though, we are here to stress a broader point: The integrated, global, decentralized communications network is vulnerable to threats that make the interception of the Speaker's telephone conversation pale by comparison. The nation's banking system and its financial markets are totally dependent on the public switched telecommunications network. So is the air traffic control system. So is the United States military. As the National Research Council recently concluded,

> "The fundamental characteristic of the PSTN [public switched telecommunications network] from the standpoint of information vulnerability is that it is a highly interconnected network of heterogeneously controlled and operated computer-based switches. Network connectivity implies that an attacker -- which might range from a foreign government to a teen-aged hacker -- can in principle connect to any network site (including sites of critical importance for the entire network) from any other network site (which may be geographically remote or even outside the United States)." Computer Science and Telecommunications Board, National Research Council, Cryptography's Role in Securing the Information Society, p. 34 (1996).

The vulnerabilities of unencrypted computer files and electronic communications are well-documented. Unencrypted communications are open to criminal exploitation, and the losses to date from inadequate system security are enormous. In one series of transactions in 1994, an international

group of criminals penetrated Citicorp's computerized electronic transfer system and moved about $12 million from legitimate customer accounts into their own accounts in banks around the world. The National Research Council recently concluded: "Of all the information vulnerabilities facing US. companies internationally, electronic vulnerabilities appear to be the most significant." Ibid.

Wireless communications should not be -- and need not be -- the weak link in the integrated communications infrastructure. Strong encryption offers opportunities for enhanced security in the digital age. Widespread use of encryption to protect communications will prevent fraud and other extremely dangerous forms of crime. At the same time, encryption poses challenges to law enforcement agencies.

The current debate over control of encryption technology is in some ways a conflict between two competing models of security, one in which private individuals, businesses and government choose from a variety of encryption options to protect their security, and one in which the government assumes primary responsibility for protecting personal and business as well as governmental security through government-mandated weaknesses in encryption technology. It has become clear to us that the centralized approach to security based on government-controlled encryption weaknesses will not work in the decentralized, competitive, globalized environment where the dynamics of decreasing cost and increasing computing power have put more control and more choices in the hands of end users.

Given these developments, there is no answer to the encryption issue that will guarantee the government access in all cases. Total prohibition is not an option. Strong non-escrowed encryption is and will continue to be available to those most committed to protecting communications, whether for legitimate or illegal purposes. There are currently hundreds of encryption products available worldwide. Other approaches that depend upon aggressive government regulation are also not viable. Government key escrow poses a level of vulnerability that is unacceptable to business and individual users, and in any event non-escrowed encryption will always be available to the committed wrongdoers.

While it is clear that most businesses and individuals will not trust the government to hold their keys, it is also becoming increasingly clear that

most encryption users, even the most sophisticated, need to be able to deal with a simple problem: if they forget or lose their own key, how do they recover their encrypted data? Addressing this problem -- responding to user needs -- has resulted in the development of a range of "key escrow," "key recovery," or "trusted third party" systems.

Privacy concerns about key escrow systems have prompted the Center for Democracy and Technology to undertake a study of key escrow. Participants in this ongoing study include the world's leading authorities in cryptography and computer security. The purpose of the study is to examine the policy and operational aspects of evolving key escrow or key management systems in terms of technical security, privacy, engineering economics, and law enforcement goals.

V. CALEA implementation poses concerns for privacy, security and cost.

Do new technologies increase or decrease the vulnerability of electronic communications to interception? The answer is both. In recognition of the difficulties posed to law enforcement by new technologies and market structures, Congress enacted the Communications Assistance for Law Enforcement Act of 1994, which requires telecommunications common carriers to ensure that their systems can satisfy law enforcement electronic surveillance requests. CALEA was intended to preserve the status quo with respect to law enforcement wiretapping abilities.

Implementation of CALEA poses serious questions. The first set of issues concern the capability requirements which are still being debated within industry forums and negotiated in sessions between industry and law enforcement. In contravention of Congress' clear intent, the FBI has argued that CALEA requires cellular telephone companies to design into their systems the capability to physically track cellular telephone users. The FBI is seeking to go beyond either preserving the status quo or taking advantage of enhancements in surveillance capability brought about by new technologies. Instead, the FBI is seeking to mandate the design of the infrastructure to expand the government's reach, which is something Congress rejected. In the same vein, the FBI is also pushing carriers for expanded availability of signaling data, an increasingly rich source of personally revealing data.

Another set of CALEA issues concern surveillance capacity. On January 14, 1997, the FBI issued a proposed notice of capacity requirements, setting forth projected levels of wireline and wireless telephone system capacity that law enforcement agencies may need in the future. The notice supersedes a highly controversial notice issued by the FBI in October 1995.* The latest notice is subject to a 30-day public comment period.

Read narrowly, the latest notice requires carriers to install a surveillance capacity that is consistent with historic patterns of law enforcement surveillance activity. However, if read a certain way, this notice would establish huge requirements, inconsistent with historic patterns of surveillance activity and perhaps exceeding even the levels in the FBI's earlier, widely criticized capacity notice. Unfortunately, the FBI has done nothing yet to dispel the broader interpretations of the second notice, and in fact has indicated informally that companies must be prepared to meet the more extensive requirements.

When it finalizes the capacity notice after the 30-day comment period, the FBI should make it clear that county-wide surveillance requirements need not be applied to every switch in a county, but rather are to be applied in light of (1) the market share of the carrier; (2) historic trends of surveillance within a county; (3) any advances in technology that reduce the burden of carrying out electronic surveillance.

VI. CALEA **mandated network security and privacy, and Congress should hold the** FCC **to the fulfillment of its responsibilities.**

Congress was concerned to ensure that the changes made to accommodate law enforcement interception in compliance with CALEA did not increase system vulnerability. Therefore, CALEA included several important security provisions. One is section 105, entitled "Systems Security and Integrity." In this provision, for the first time ever, Congress mandated that telecommunications companies "shall ensure" that interceptions within their switching systems can occur only upon the affirmative intervention of an individual officer of or employee of the carrier. Section 103(a)(4) of

---

* In the October 1995 notice, it seemed that law enforcement was seeking the capacity to intercept up to 1% of telephone lines in major urban areas.

CALEA requires companies to ensure that systems are designed "In a manner that protects the privacy and security of communications . . . not authorized to be intercepted. Finally, section 301 of CALEA requires the Federal Communications Commission to issue regulations governing system security. We urge the Committee to ensure that the FCC is carrying out these provisions.

VII. The FCC should exercise its authority to ensure the promotion of telecommunications system security.

Concerns with network security go beyond CALEA. The FCC has both the authority and the responsibility under section 1 of the Communications Act, 47 U.S.C. 151 to ensure the security and reliability of the nation's communications networks. In the past, this Subcommittee has paid particular attention to reliability concerns in the public switched telephone network. In an increasingly decentralized and complex system, full attention to network security issues requires a broad look at the network security features available to users, including flexible and robust encryption. We urge the Subcommittee to work with the Commission on this pressing concern.

Conclusions

Congress should assure that current laws adequately protect privacy in light of ongoing developments in telecommunications technology. Wireless data transfers should be brought explicitly within ECPA. The international implications of global communications privacy should be addressed. A new encryption policy should be developed that defers to user-driven solutions. The Subcommittee should examine the FCC's oversight of network security and its response to the network security provisions of CALEA.

We would be happy to work with the Subcommittee to accomplish these goals.

Rule 4(b)(2) Statement

Neither Jerry Berman nor the Center for Democracy and Technology has received any Federal grant, or subgrant thereof, nor any Federal contract, or subcontract thereof, during the current fiscal year or either of the two preceding fiscal years.